(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 198 37 642 C 1**

(51) Int. Cl.[6]:
G 06 F 3/02
G 06 F 12/14
G 07 C 9/00
H 04 M 1/66
H 04 B 1/38
G 06 K 9/52

(21) Aktenzeichen: 198 37 642.1-53
(22) Anmeldetag: 19. 8. 98
(43) Offenlegungstag: -
(45) Veröffentlichungstag der Patenterteilung: 25. 11. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

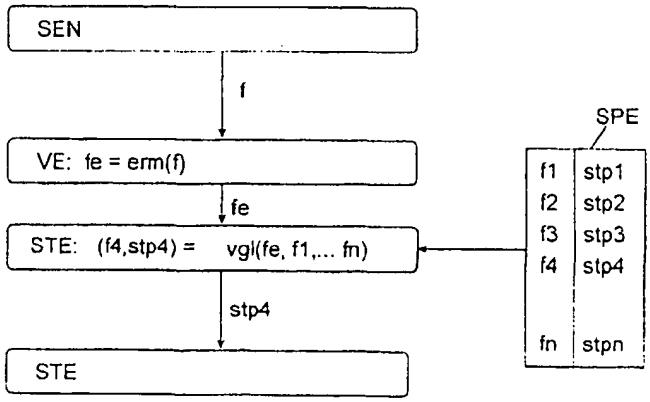
(73) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Raaf, Bernhard, Dipl.-Phys., 81475 München, DE;
Bromba, Manfred, Dr.rer.nat., 81669 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 196 45 937 A1
US 57 64 222

(54) Verfahren und Anordnung zur Steuerung eines Gerätes mittels Fingerabdruckinformationen

(57) Die Steuerung eines Gerätes erfolgt in Abhängigkeit von durch einen Sensor ermittelten Fingerabdruckinformationen, die mit gespeicherten, unterschiedlichen Fingern einer Person entsprechenden Fingerabdruckinformationen verglichen werden, denen jeweils eine Steuerprozedur zugeordnet ist.



DE 198 37 642 C 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren und eine Anordnung zur Steuerung eines Gerätes, insbesondere eines mobilen Gerätes, mittels Fingerabdruckinformationen, wobei das Gerät im Wesentlichen durch das Anlegen unterschiedlicher Fingerabdrücke gesteuert wird, bzw. die Eingabe von Steuerinformationen mittels unterschiedlicher Fingerabdrücke erfolgt.

Zur Eingabe von Steuerinformationen in mobile Geräte sind bislang mehrere verschiedene Verfahren, wie beispielsweise mittels Tastatur, Softkeys, Spracherkennung, Maus, Joystick oder Touchscreen bekannt.

Diese bekannten Verfahren weisen entweder den Nachteil auf, daß sie, insbesondere in mobilen Geräten, zu einer unerwünscht aufwendigen Realisierung eines Gerätegehäuses führen, oder daß sie unzuverlässig sind, bzw. ihre Durchführung viel Rechenaufwand und somit auch Energieaufwand erfordert.

Außerdem ist eine Vielzahl von Geräten bekannt, vor deren Benutzung ein Benutzer sich authentifizieren muß. Wichtige Beispiele sind Computer, insbesondere tragbare Computer, und Telekommunikationsgeräte, insbesondere Mobiltelefone.

Einige Geräte sind dabei generell gegen unberechtigte Benutzung beispielsweise durch ein Paßwort geschützt; bei anderen Geräten sind lediglich bestimmte Funktionen vor unberechtigtem Zugriff (beispielsweise durch eine sogenannte Personal Identification Number PIN) geschützt. Hierzu gehört auch der Schutz des Zugangs zu bestimmten Daten oder Diensten, auch wenn diese nicht durch das Gerät, sondern durch andere Geräte in einem Computer- oder Kommunikationsnetz wie beispielsweise einem Mobilfunksystem zur Verfügung gestellt werden.

Die heute wohl häufigste Art der Eingabe einer Authentifikationsinformation bzw. Authentifizierungsinformation ist die Eingabe über eine Tastatur des Gerätes. Nach der Eingabe wird die Richtigkeit der eingegebenen Information, und damit die Berechtigung des eingebenden Benutzers durch eine Prüfeinrichtung im Gerät oder in einem Computer oder Kommunikationsnetz geprüft. Bei Mobiltelefonen nach dem GSM (Global System for Mobile Communication)-Standard geschieht dies, indem eine Datenverarbeitungseinrichtung auf der sogenannten SIM (Subscriber Identifying Module)-Card des Gerätes prüft, ob die eingegebene PIN zu der auf der SIM-Card gespeicherten Information paßt. Ist dies der Fall, gibt die SIM-Card das Mobiltelefon zur Benutzung frei.

Seit einiger Zeit sind Technologien verfügbar, die andere Formen der Authentifikation eines Benutzers erlauben. Diese Technologien beruhen auf der Erfassung benutzerspezifischer biometrischer Merkmale durch spezielle Sensoren. Ein wichtiges Beispiel hierfür sind Sensoren zur Erkennung des Fingerabdruckes.

Üblicherweise werden die von den Sensoren erfaßten Merkmale in einer Datenverarbeitungseinrichtung des Gerätes oder eines Kommunikationsnetzes mit den bekannten Merkmalen eines berechtigten Benutzers verglichen und bei hinreichender Übereinstimmung wird der Zugang zu dem gewünschten Dienst, den benötigten Daten oder der gewählten Gerätefunktion freigeschaltet.

Obwohl diese Geräte zur Benutzerauthentifizierung bereits ein Eingabemittel, nämlich einen entsprechenden Sensor, aufweisen, sind sie dennoch mit einer Tastatur oder einer entsprechenden Eingabevorrichtung versehen, mittels derer ein Benutzer Steuerinformationen oder Eingabeinformationen eingeben kann.

Aus der Druckschrift DE 196 45 937 A1 ist bekannt: ein

Verfahren zur Steuerung eines Gerätes mittels Fingerabdruckinformationen, bei dem

- Fingerabdruckinformationen eines Fingers ermittelt werden,
- entsprechend jeweils einem Finger verschiedener Personen unterschiedliche Fingerabdruckinformationen gespeichert sind, denen jeweils eine Steuerprozedur zugeordnet ist,
- die ermittelten Fingerabdruckinformationen mit den gespeicherten Fingerabdruckinformationen verglichen werden,
- bei einer einen vorgegebenen Schwellwert überschreitenden Ähnlichkeit der ermittelten Fingerabdruckinformationen mit gespeicherten Fingerabdruckinformationen die diesen Fingerabdruckinformationen zugeordnete Steuerprozedur ausgelöst wird.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Anordnung anzugeben, mit denen es möglich ist, auf zuverlässige und einfache Weise Steuerinformationen zur Steuerung eines Gerätes einzugeben, ohne auf der Außenseite eines Gerätegehäuses viel Platz zu benötigen, oder das Gerätegewicht wesentlich zu erhöhen.

Diese Aufgabe wird durch die Merkmale der unabhängigen Patentansprüche gelöst. Weiterbildungen ergeben sich aus den Unteransprüchen.

Die Erfindung beruht also auf dem Gedanken, Fingerabdruckinformationen eines angelegten Fingers zu ermitteln, diese mit unterschiedlichen gespeicherten Fingerabdruckinformationen zu vergleichen, und in Abhängigkeit von dem Vergleichsergebnis das Gerät zu steuern.

Die Erfindung unterscheidet sich vom Stand der Technik insbesondere darin, daß verschiedene Finger einer Person anhand des Fingerabdrucks erkannt werden und jedem dieser Finger eine eigene Steuerprozedur zugeordnet ist.

Dadurch wird erreicht, daß mittels eines in der Fläche relativ kleinen Sensors entsprechend den unterschiedlichen Fingern unterschiedliche Steuerinformationen eingegeben werden können. So können entsprechende Geräte bzw. die zugeordneten Eingabevorrichtungen klein und leicht gehalten werden, und gleichzeitig die Eingabe der Steuerinformation sehr zuverlässig durchgeführt werden.

Bei einer Weiterbildung der Erfindung ist vorgesehen, daß auch eine Benutzererkennung oder eine Benutzerauthentifizierung mittels einer Fingerabdruckerkennung erfolgt.

So ist es möglich, mit einem Fingerabdrucksensor das Gerät vor unberechtigtem Zugriff zu schützen, und im Falle eines berechtigten Gerätezugriffs das Gerät ohne zusätzlichen Hardwareaufwand auch zu steuern.

Ferner ist eine Weiterbildung vorgesehen, bei der durch das Anlegen unterschiedlicher Finger entsprechende unterschiedliche Ziffern in das Gerät eingegeben werden können.

Dadurch wird erreicht, daß durch den Einsatz eines Sensors anstelle einer numerischen Tastatur ein Gerät zuverlässig bedient werden kann, es aber in seinen Abmessungen und seinem Gewicht klein gehalten werden kann.

Eine weitere Ausgestaltung der Erfindung sieht vor, daß das Anlegen eines Fingers in unterschiedlichen Betriebszuständen unterschiedliche Steuerprozeduren im Gerät auslöst.

So ist es möglich, daß mit einer beschränkten Anzahl unterschiedlicher Finger eine große Anzahl von Steuerprozeduren im Gerät ausgelöst werden kann.

Insbesondere in Kommunikationsendgeräten kann mittels unterschiedlicher Finger auf schnelle und zuverlässige Weise die Eingabe von Wahlinformationen erfolgen bzw.

die Auslösung der zugehörigen Signalisierungsprozeduren ausgelöst werden.

Die Erfindung wird im Folgenden anhand bevorzugter Ausführungsbeispiele näher beschrieben, zu deren Erläuterung die nachstehend aufgelisteten Figuren dienen:

Fig. 1 ein Flußdiagramm eines Verfahrens und die entsprechenden Anordnungselemente zur Steuerung eines Gerätes mittels Fingerabdruckinformation,

Fig. 2 mögliche Zuordnungen von Fingerabdruckinformationen zu Steuerprozeduren,

Fig. 3 ein Blockschaltbild eines Kommunikationsendgerätes.

Fig. 1 zeigt ein Flußdiagramm eines Verfahrens zur Steuerung eines Gerätes mittels unterschiedlicher Fingerabdruckinformationen und entsprechende Anordnungselemente zur Durchführung eines derartigen Verfahrens.

Zunächst erfaßt ein Fingerabdrucksensor SEN das Linienmuster f der angelegten Fingerkuppe, indem die Sensorzellen die Änderungen des elektrischen Feldes, das die erhobenen Linien und die Vertiefungen auf der Fingeroberfläche hervorrufen aufnehmen, und daraus sein elektrisches Abbild erzeugen.

Die Erfassung kann dabei auf einem kapazitiven Meßprinzip beruhen, bei dem jedes Pixel einen Kondensator darstellt und die Haut des aufgelegten Fingers als dritte Kondensatorplatte wirkt. Die sich durch die Erhöhungen und Vertiefungen in den einzelnen Sensorelementen ergebenden Rückkoppelungskapazitäten ergeben analoge Werte, die eine dreidimensionale Aufnahme des Abdrucks liefern. Da überdies die Leitfähigkeit der Haut das Signal beeinflußt, ist der Sensor auch mit einer Wachsatrappe nicht zu täuschen.

Nach einer Analog-/Digitalwandlung dieser analogen Werte werden die entsprechenden digitalen Signale an eine Verarbeitungseinrichtung VE, insbesondere einen digitalen Signalprozessor übermittelt.

Im digitalen Signalprozessor VE werden durch geeignete Bildverarbeitungsalgorithmen aus den Fingerabdruckswerten f unverwechselbare Merkmale fe errechnet fe = erm(f). Diese ermittelten unverwechselbaren Merkmale fe werden in einer Steuereinrichtung STE, wie einem Mikrocontroler, mit entsprechenden gespeicherten unverwechselbaren Merkmalen f1, ... fn, die in Speicherbausteinen SPE abgespeichert sind, verglichen: (f4, stp_4) = vgl(fe, f1, ... fn); in Abhängigkeit von dem Vergleichsergebnis wird dann bei vorliegender Ähnlichkeit gespeicherter Fingerabdruckinformationen f4 mit den ermittelten Fingerabdruckinformationen fe die diesen gespeicherten Fingerabdruckinformationen f4 zugeordnete Steuerprozedur stp4 ausgelöst.

Die gespeicherten Fingerabdruckinformationen entsprechen dabei entweder unterschiedlichen Fingern einer Person, oder unterschiedlichen Fingern mehrerer Personen. So können beispielsweise entweder für eine Person die den zehn Fingern entsprechenden Fingerabdruckinformationen abgespeichert sein, oder zusätzlich für jede weitere Person die entsprechenden den zusätzlichen zehn Fingern entsprechenden weiteren Fingerabdruckinformationen abgespeichert sein.

Für eine zuverlässige Untersuchung hinsichtlich ihrer Ähnlichkeit können die von der Sensoreinrichtung SEN erfaßten und die gespeicherten Fingerabdruckinformationen in die Form eines sogenannten Merkmalsvektors gebracht werden. Diese Annahme ist in der Praxis keine Einschränkung, da die Sensordaten stets als geordnetes n-Tupel von n Meßdaten (Merkmalsvektor) dargestellt werden können. Die Merkmalsvektoren bilden einen n-dimensionalen Raum. In diesem existiere ein Satz von Mustervektoren (Codebuchvektoren), und es sei ein Abstandsmaß (Ähnlichkeitsmaß für Fingerabdruckmerkmale) definiert.

Zu jedem Mustervektor gibt es eine Zelle in diesem Raum, die dadurch definiert ist, daß für jeden Merkmalsvektor in einer Zelle gilt, daß der Mustervektor dieser Zelle der nächstgelegene Mustervektor im Sinne dieses Abstandsmaßes ist.

Jedem Mustervektor sei eine Steuerprozedur zur Steuerung des Gerätes oder eine entsprechende Information zur Auslösung einer derartigen Steuerprozedur zugeordnet. Die Ermittlungen des nächstgelegenen Mustervektors f4 zu einem Merkmalsvektor fe, der den erfaßten Sensordaten entspricht, führt damit zur Auslösung einer entsprechenden Steuerprozedur stp4, die durch obenerwähnte erste oder eine zweite Steuereinrichtung STE ausgeführt werden kann. Falls der Merkmalsvektor nicht in der Zelle eines Mustervektors liegt, wird keine Steuerprozedur ausgelöst, da die Ähnlichkeit zwischen ermittelten und gespeicherten Fingerabdruckinformationen zu gering ist, d. h. die Ähnlichkeit eine vorgegebene Schwelle nicht überschreitet.

Die Fehlerraten dieses Verfahrens lassen sich optimieren, wenn sichergestellt ist, daß die mit den Fingerabdruckmerkmalen assoziierten Merkmalsvektoren Mustervektoren sind. Dies läßt sich erreichen, indem das System sich in einer Initialisierungsphase an die Fingerabdruckmerkmale adaptiert (Codebuchadaption).

Die Vektorquantisierung ist nicht das einzige Verfahren, das im Zusammenhang mit der Erfindung eingesetzt werden kann. Dem Fachmann sind andere Verfahren geläufig, die deshalb hier nicht erläutert werden müssen.

Die Speicherung von Fingerabdruckinformationen, die Verarbeitung von Fingerabdruckinformationen, der Vergleich von ermittelten und gespeicherten Fingerabdruckinformationen und/oder die Auslösung von Steuerprozeduren kann entweder ganz oder zumindest teilweise in einer Anordnung zur Steuerung eines Gerätes erfolgen. Diese Anordnung zur Steuerung kann in dem Gerät integriert sein oder separat vom Gerät realisiert sein und nur mittels Übertragungseinrichtungen mit dem Gerät verbunden sein. Es ist auch möglich, daß Teile der oben erwähnten Verfahrensschritte bzw. der entsprechenden Hardwareelemente in zentralen Einrichtungen eines Kommunikationsnetzes durchgeführt werden bzw. angeordnet sind.

In **Fig.** 2 sind unterschiedliche Varianten für die Zuordnung von Fingerabdruckinformationen zu Steuerprozeduren schematisch dargestellt. Sie beziehen sich auf ein Gerät, das in unterschiedliche Betriebszustände versetzt werden kann. Die unterschiedlichen Betriebszustände können sich dabei darin unterscheiden, daß je nach Betriebszustand unterschiedliche bzw. mehr oder weniger Elemente des Gerätes mit Strom versorgt sind, unterschiedliche bzw. mehr oder weniger Funktionen des Gerätes ausführbar sind, oder ein mehr oder weniger eingeschränkter Zugriff auf Daten oder Funktionen zugelassen ist. Dabei kann durch das Anlegen eines Fingers an das Sensorelement SEN die diesem Fingerabdruck zugeordnete Steuerprozedur zum Wechsel des Betriebszustandes des Gerätes führen.

Im folgenden sind die drei in **Fig.** 2 von links nach rechts exemplarisch dargestellten Abläufe näher beschrieben:

- Das Gerät befindet sich zunächst im ausgeschalteten Zustand aus, in dem nur die Elemente zur Fingerabdruckerkennung eingeschaltet sind. Entsprechen die ermittelten Fingerabdruckinformationen fe den gespeicherten Fingerabdruckinformationen f1, so wird das Gerät mittels der Steuerprozedur stp1 eingeschaltet und für eine bestimmte Person person1 freigeschaltet. Das heißt im Sinne einer Benutzerauthentifizierung oder Benutzererkennung werden dieser Person person1 die ihr entsprechenden Zugriffe auf das Gerät gestattet.

Wird im nächsten Schritt wieder der Fingerabdruck f1 er-

kannt, so wird das Gerät mittels Steuerprozedur stp113 in das Geräteprofil profil1 geschaltet. Dies kann bedeuten, daß beispielsweise bei einem Kommunikationsendgerät die Rufton lautstärke, die Zulässigkeit ankommender Rufe, die Rufton melodie, die Displaydarstellung oder andere Menüoptionen gemäß diesem abgespeicherten Geräteprofil profil1 eingestellt werden.

Wird nun in diesem Geräteprofil profil1 nochmals der Finger f1 angelegt, so wird automatisch die gespeicherte Rufnummer eines gewünschten Ziels, wie beispielsweise des Büros des Nutzers, eingegeben und entsprechende Signalisierungsprozeduren zum Aufbau der Verbindung eingeleitet: waehle_buero.

- Wird im ausgeschalteten Zustand festgestellt, daß der ermittelte Fingerabdruck fe dem gespeicherten Fingerabdruck f68 entspricht, so wird das Gerät eingeschaltet und für eine Person person2 freigeschaltet. Wird als nächstes der Fingerabdruck f69 erkannt, so wird das Gerät auf das Geräteprofil profil3 dieser Person person2 geschaltet. Wird nun der Fingerabdruck f30 erkannt, so wird automatisch ein Verbindungsaufbau zu einer Notrufzentrale eingeleitet.

- Wird im ausgeschalteten Gerätezustand der Fingerabdruck f27 erkannt, so wird das Gerät zunächst eingeschaltet und sofort ein Verbindungsaufbau zu einer Notrufzentrale eingeleitet. Wird dann im eingeschalteten Zustand der Finger f24 erkannt, wird das Gerät auf ein allgemeines Geräteprofil profil1 geschaltet und im Falle des Anlegens des Fingers f21 die Ziffer "0" am Gerät eingegeben und ggf. auf dem Display dargestellt.

Anhand dieser Beispiele sind für einen Fachmann unzählige andere Varianten der Zuordnung von Steuerprozeduren zu Fingerabdruckinformationen realisierbar.

Eine derartige Zuordnung kann beim erstmaligen Benutzen des Gerätes abgespeichert werden, indem der Benutzer nacheinander alle Optionen der Menüstruktur zur Steuerung des Gerätes auswählt und jeden Menüpunkt mit dem Anlegen des von ihm gewünschten Fingers an den Sensor bestätigt.

Im Zusammenspiel mit einer im Gerät bzw. in der Anordnung zur Steuerung des Gerätes vorhandenen SIM (Subscriber Identifying Module)-Card kann der Fingerabdrucksensor nicht nur zur Benutzererkennung, sondern auch zur Benutzerauthentifizierung dienen.

Fig. 3 zeigt ein Kommunikationsendgerät KE, bestehend aus einer Bedieneinheit MMI, einer Steuereinrichtung STE, einer Verarbeitungseinrichtung VE, einer Stromversorgungseinrichtung SVE, einem Benutzerauthentifizierungsmodul SIM, einer Empfangseinrichtung EE, einer Sendeeinrichtung SE und einer Sensoreinrichtung SEN.

Die Bedieneinheit MMI besteht aus einem Lautsprecherelement, einem Mikrofonelement, einem Display zur Darstellung von Menüpunkten, Ziffern oder anderer für einen Kommunikationsablauf relevanter Informationen und ggf. einer Tastatur zur Eingabe von Ziffern und Buchstaben und zur Auswahl von Menüpunkten.

Die Steuereinrichtung STE besteht im wesentlichen aus einem programmgesteuerten Mikrocontroler und die Verarbeitungseinrichtung VE aus einem digitalen Signalprozessor, wobei beide schreibend und lesend auf Speicherbausteine SPE zugreifen können. Der Mikrocontroler steuert und kontrolliert alle wesentlichen Elemente und Funktionen des Kommunikationsendgerätes KE und steuert den Kommunikations- und Signalisierungsablauf. Dazu werden in Form von Programmdaten gespeicherte Steuerprozeduren aus den Speicherbausteinen in den Mikrocontroler gelesen und dort ausgeführt. Insbesondere die Versetzung des Kommunikationsendgerätes KE in definierte Betriebszustände, das Ein- und Ausschalten bestimmter Hardwareelemente und die Benutzererkennung werden durch die Steuereinrichtung STE gesteuert.

In den flüchtigen oder nichtflüchtigen Speicherbausteinen SPE sind die Programmdaten, die zur Steuerung des Kommunikationsendgerätes KE und des Kommunikationsablaufs, insbesondere auch der Signalisierungsprozeduren benötigt werden, Geräteinformationen, vom Nutzer eingegebene Informationen, während der Verarbeitung von Signalen entstehende Informationen und Referenzdaten von Fingerabdruckmerkmalen, also Fingerabdruckinformationen von berechtigten Benutzern, abgespeichert.

Bei einer Ausführungsvariante der Erfindung sind diese Referenzdaten oder zumindest Teile dieser Referenzdaten auf dem Benutzerauthentifizierungsmodul SIM abgespeichert.

Handelt es sich bei dem Kommunikationsendgerät KE um ein Mobiltelefon, so kann die Benutzerauthentifizierung mittels Geheimzahl durch den Vergleich der ermittelten Fingerabdruckinformationen mit abgespeicherten Fingerabdruckinformation ersetzt werden. Nach einer Übermittlung entsprechender Authentifizierungsdaten zu zentralen Einrichtungen des Mobilfunksystems wird das Mobiltelefon in das Mobilfunksystem eingebucht.

Patentansprüche

1. Verfahren zur Steuerung eines Gerätes mittels Fingerabdruckinformationen, bei dem
   - Fingerabdruckinformationen (fe) eines Fingers ermittelt werden,
   - entsprechend unterschiedlichen Fingern einer Person unterschiedliche Fingerabdruckinformationen (f1; f2; ... fn) gespeichert sind, denen jeweils eine Steuerprozedur (stp1; stp2; ... stpn) zugeordnet ist,
   - die ermittelten Fingerabdruckinformationen (fe) mit unterschiedlichen gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) verglichen werden,
   - bei einer einen vorgegebenen Schwellwert überschreitenden Ähnlichkeit der ermittelten Fingerabdruckinformationen (fe) mit gespeicherten Fingerabdruckinformationen (f4) die diesen gespeicherten Fingerabdruckinformationen (f4) zugeordnete Steuerprozedur ausgelöst wird.
2. Verfahren nach Anspruch 1, bei dem das Gerät in unterschiedliche Betriebszustände versetzt werden kann, wobei gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) eine Steuerprozedur (stp1; stp2; ... stpn) zum Wechsel des Betriebszustandes zugeordnet ist.
3. Verfahren nach einem der vorhergehenden Ansprüche, bei dem gespeicherten Fingerabdruckinformationen (f1) eine Steuerprozedur (stp1) zur Durchführung einer Benutzererkennung zugeordnet ist.
4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) Steuerprozeduren (stp1; stp2; ... stpn) zugeordnet sind, deren Auslösungen der Eingabe von Ziffern entsprechen.
5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das Gerät in unterschiedliche Betriebszustände versetzt werden kann, wobei gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) in unterschiedlichen Betriebszuständen unterschiedliche Steuerprozeduren (stp1; stp2; ... stpn) zugeordnet sind.
6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem es sich bei dem Gerät um ein Kommuni-

kationsendgerät handelt, wobei gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) Steuerprozeduren (stp1; stp2; ... stpn) zugeordnet sind, deren Auslösungen der Eingabe von Wahlinformationen entsprechen.

7. Verfahren nach einem der vorhergehenden Ansprüche, bei dem es sich bei dem Gerät um ein Kommunikationsendgerät handelt, wobei gespeicherten Fingerabdruckinformationen (f1; f2; ... fn) Steuerprozeduren (stp1; stp2; ... stpn) zugeordnet sind, deren Auslösungen Signalisierungsprozeduren auslösen.

8. Anordnung zur Steuerung eines Gerätes mittels Fingerabdruckinformationen mit

a) Mitteln (SEN) zur Ermittlung von Fingerabdruckinformationen (fe),

b) Mitteln (SPE) zur Speicherung unterschiedlicher Finger einer Person entsprechender unterschiedlicher Fingerabdruckinformationen (f1; f2; ... fn), denen jeweils eine Steuerprozedur (stp1; stp2; ... stpn) zugeordnet ist,

c) Mitteln (STE) zum Vergleich der ermittelten Fingerabdruckinformationen (fe) mit unterschiedlichen gespeicherten Fingerabdruckinformationen (f1; f2; ... fn), und

d) Mitteln (STE) zur Auslösung der Steuerprozedur (stp4), die den gespeicherten Fingerabdruckinformationen (f4) zugeordnet ist, deren Ähnlichkeit mit den ermittelten Fingerabdruckinformationen (fe) einen vorgegebenen Schwellwert überschreitet.

9. Anordnung nach Anspruch 8, mit

- Mitteln (STE) zur Versetzung des Gerätes in unterschiedliche Betriebszustände,
- mit Mitteln (SPE) zur Speicherung einer Steuerprozedur (stp1) zum Wechsel des Betriebszustandes.

10. Anordnung nach einem der Ansprüche 8 bis 9, mit Mitteln (SPE) zur Speicherung einer Steuerprozedur (stp8) zur Durchführung einer Benutzererkennung.

11. Anordnung nach einem der Ansprüche 8 bis 10, mit Mitteln (SPE) zur Speicherung von Steuerprozeduren (stp1; stp2; ... stpn), deren Auslösungen der Eingabe von Ziffern entsprechen.

12. Anordnung nach einem der Ansprüche 8 bis 11, mit Mitteln (SPE) zur Speicherung von Steuerprozeduren (stp1; stp2; ... stpn), deren Auslösungen der Eingabe von Wahlinformationen entsprechen.

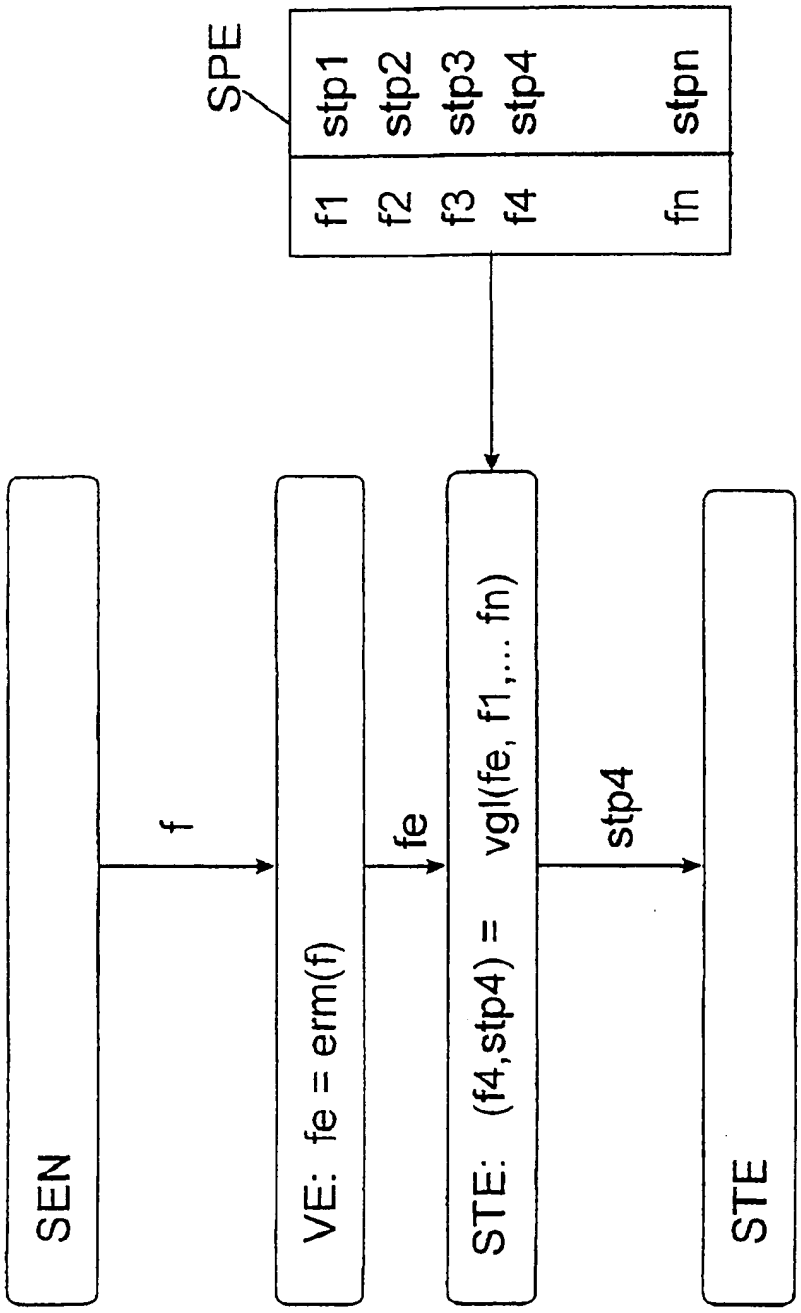
13. Anordnung nach einem der Ansprüche 8 bis 12, mit Mitteln (SPE) zur Speicherung von Steuerprozeduren (stp1; stp2; ... stpn), deren Auslösungen Signalisierungsprozeduren auslösen.

14. Mobiltelefon mit einer Anordnung nach einem der Ansprüche 8 bis 13.

Hierzu 3 Seite(n) Zeichnungen

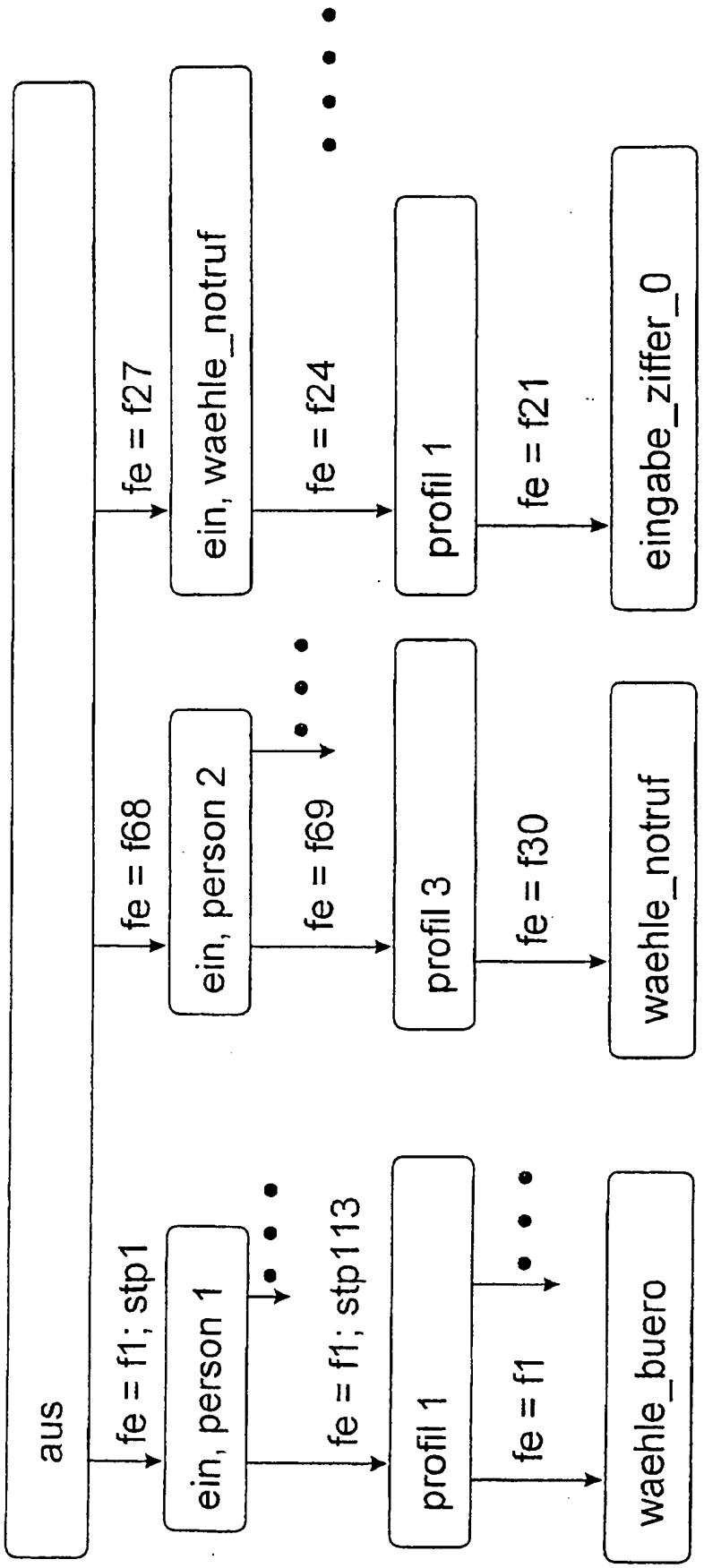
Nummer: DE 198 37 642 C1
Int. Cl.[6]: G 06 F 3/02
Veröffentlichungstag: 25. November 1999

FIG 1



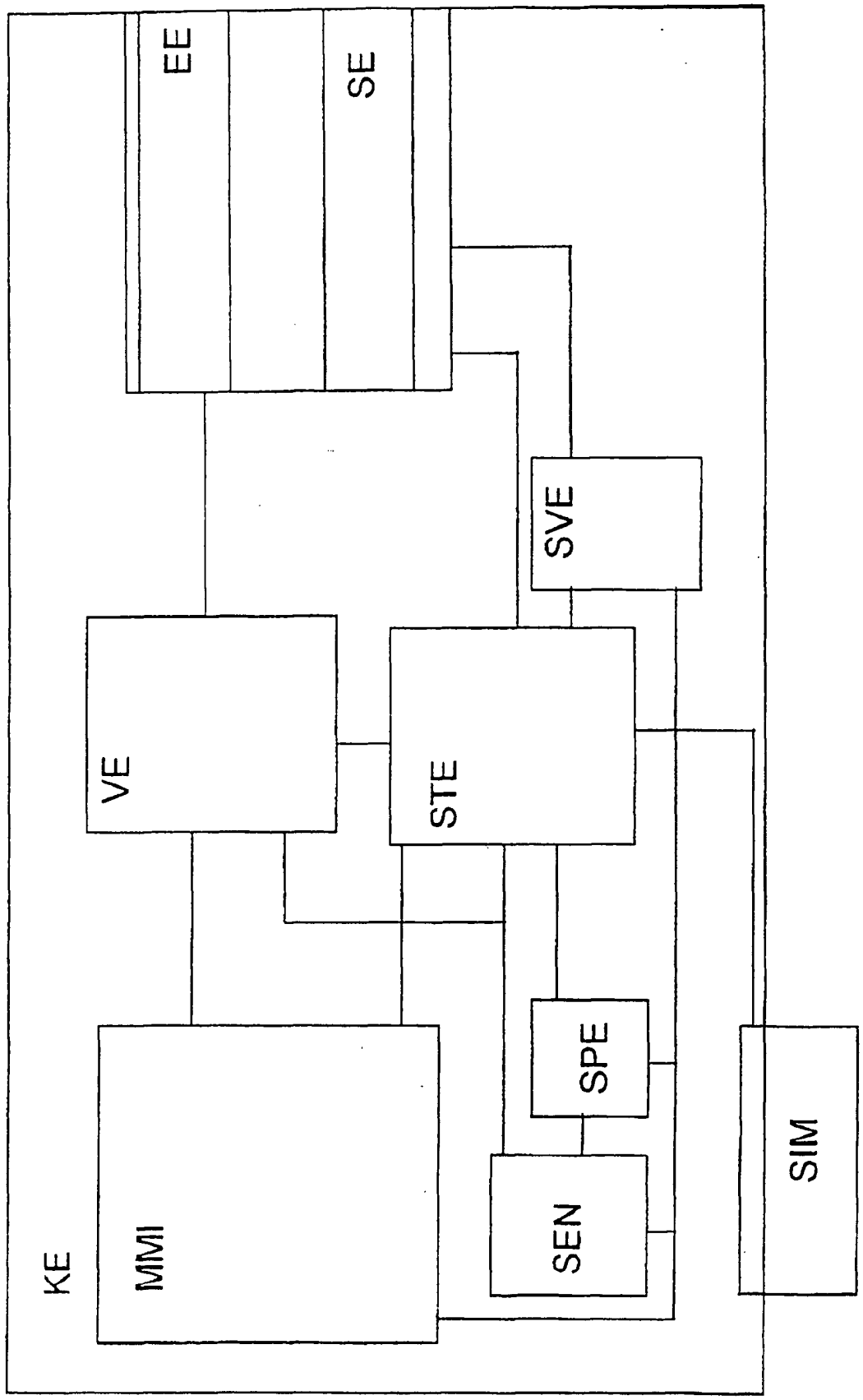
Nummer: DE 198 37 642 C1
Int. Cl.[6]: G 06 F 3/02
Veröffe. ..chungstag: 25. November 1999

FIG 2



Nummer: DE 198 37 642 C1
Int. Cl.[6]: G 06 F 3/02
Veröffentlichungstag: 25. November 1999

FIG 3



(19) **FEDERAL REPUBLIC OF GERMANY**

(12) **Unexamined Patent Application**
(10) **DE 198 37 642 C1**

(51) Int. Cl. [6]:
G 06 F 3/02
G 06 F 12/14
G 07 C 9/00
H 04 M 1/66
H 04 B 1/38
G 06 K 9/52

GERMAN PATENT OFFICE

(21) File Number: 198 37 642, 1-53
(22) Date of Filing: 19. 8. 98
(43) Date of Publication: --
(45) Date of Publication by Printing of a GrantedPpatent : 25. 11. 99

Opposition may be filed within 3 months after publication of the patent grant.

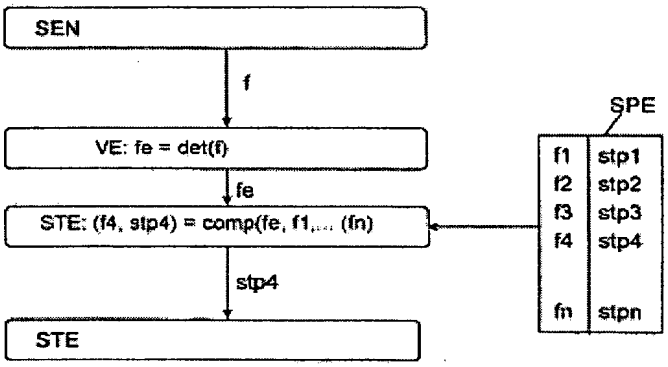
(73) Assignee:
Siemens AG, 80333 Munich, DE

(72) Inventor:
Raaf, Bernhard, Dipl.-Phys., 81475 Munich, DE;
Bromba, Manfred, Dr.rer.nat., 81669 Munich, DE

(56) Documents considered in determining patentability:
DE 196 45 937 A1
US 57 64 222

(54) Method and Arrangement for Controlling a device by means of Fingerprint Information

(57) A device is controlled as a function of fingerprint information determined by means of a sensor, the information being compared to stored fingerprint information corresponding to the different fingers of a person, each of which is associated with a control procedure.



Specification

The invention relates to a method and an arrangement for controlling a device, particularly a mobile device, by means of fingerprint information, the device being controlled substantially by applying various fingerprints or the input of control information occurring by means of various fingerprints.

To input control information in mobile devices so far several different methods are known, such as the use of keypads, soft keys, speech recognition, a mouse, joystick or a touch screen.

These familiar methods either have the disadvantage that they lead to undesirably complex implementation of the housing for the device, particularly in the case of mobile devices, or that they are unreliable, and/or that their implementation necessitates extensive computation and hence also energy.

Moreover a variety of devices are known, which require a user to identify himself prior to use. Important examples are computers, particularly portable computers, and telecommunication devices, particularly mobile telephones.

Some devices are completely protected from unauthorized use, for example by means of a password; in other devices only certain functions are protected from unauthorized access (for example by means of a so-called personal identification number, or PIN). This includes also the protection of access to certain data or services, even if these are not provided by the device, but are made available by other devices in a computer or communication network, for example a cellular phone system.

Today probably the most common way of inputting authentication information is input by means of a keypad of the device. After input has occurred, the accuracy of the input information, and consequently the authorization of the inputting user, is verified by means of a test system in the device or in a computer or communication network. In the case of cellular phones based on the GSM (Global System for Mobil Communication) standard this occurs in that a data processing device located on the so-called SIM (Subscriber Identification Module) card of the device verifies whether the input PIN corresponds to the information stored on the SIM card. If this is the case, the SIM card releases the cellular phone for use.

For quite some time, technologies have been available that allow other types of user authentication. These technologies are based on the detection of user-specific biometric features by means of special sensors. Important examples of this are sensors used to recognize fingerprints.

The features detected by the sensors are typically compared to the known features of an authorized user by a data processing mechanism in the device or on a communication network, and if they sufficiently agree, access is granted to the desired service, the required data or the selected device function.

Although these user authentication devices already comprise an input means, namely a corresponding sensor, they also comprise a keypad or a corresponding input device, by means of which a user may input control information or other input information.

DE-19645937-A1 discloses a method for controlling a device by means of fingerprint information wherein

- fingerprint information of a finger is determined,
- different pieces of fingerprint information corresponding to one finger each of various persons is stored, each piece of information being associated with a control procedure,
- the determined fingerprint information is compared to the stored fingerprint information, and
- in case a similarity of the determined fingerprint information with the stored fingerprint information is achieved that exceeds a defined threshold value the control procedure associated with this fingerprint information is triggered.

It is therefore the object of the invention to provide a method and an arrangement, which make it possible to input control information reliably and easily for the purpose of controlling a device, without requiring a lot of space exterior to the device housing or increasing the weight of the device significantly.

This object is achieved with the features of the independent patent claims. Further embodiments are disclosed in the dependent claims.

The invention is based on the idea of determining the fingerprint information of an applied finger, comparing it to stored fingerprint information of different fingers, and controlling the device as a function of the result of the comparison.

The invention differs from the prior art particularly in that different fingers of one person are recognized based on the fingerprint and that each of these fingers is associated with a specific control procedure.

This way, different pieces of control information can be input by means of a relatively small sensor in terms of its surface, the pieces of information corresponding to the different fingers. Corresponding devices and/or the associated input devices can therefore be kept small and lightweight, and at the same time the control information can be input very reliably.

In a further development of the invention further provides for user recognition or user authentication being performed based on fingerprint recognition.

This way, using a fingerprint sensor, it is possible to protect the device from unauthorized access and also to control the device without additional hardware expenses when access to the device has been authorized.

Additionally a further development is provided, wherein different figures can be input to the device by applying different fingers.

By using a sensor instead of a numerical keypad a device can be operated reliably, yet the dimensions and the weight thereof can be kept small.

Another embodiment of the invention provides that the application of a finger in varying operating modes triggers different control procedures in the device.

It is therefore possible to trigger a large number of control procedures in the device with a limited number of different fingers.

Particularly in communication terminals, the selected information can be input and/or the corresponding signaling

procedures can be triggered quickly and reliably by means of different fingers.

The invention will be explained in more detail hereinafter with reference to the preferred embodiments that are illustrated in the figures below, wherein:

Fig. 1 is a flow chart of a method and the corresponding arrangement elements for controlling a device by means of fingerprint information,

Fig. 2 shows possible associations of fingerprint information with control procedures,

Fig. 3 is a block diagram of a communication terminal.

Fig. 1 shows a flow chart of a method for controlling a device by means of different fingerprint information and corresponding arrangement elements for executing such a method.

A fingerprint sensor SEN first captures the line pattern 'f' of the applied fingertip in that the sensor cells detect the changes in the electric field created by the raised lines and the indentations on the finger surface, and from this generates an electric image thereof.

The detection can be based on a capacitive measurement principle, in which every pixel represents a capacitor and the skin of the applied finger acts as a third capacitor plate. The feedback capacities resulting from the elevations and indentations in the individual sensor elements result in analog values, which provide a three-dimensional image of the print. Since the conductivity of the skin further influences the signal, the sensor moreover cannot be deceived by a mock wax copy.

After this analog-to-digital conversion of these analog values, the corresponding digital signals are transmitted to a processing unit 'VE', particularly a digital signal processor.

In the digital signal processor 'VE', distinctive features 'fe' are derived from the fingerprint values 'f' by means of calculation 'fe = det(f)' using suitable image processing algorithms. These determined distinctive features 'fe' are compared to corresponding stored distinctive features 'f1...fn', which have been stored in memory modules 'SPE', in a control device 'STE' such as a micro-controller: '(f4, stp 4) = comp(fe, f1...fn)'; then, as a function of the results of the comparison, when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe', the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered.

The stored pieces of fingerprint information correspond either to different fingers of a person or to different fingers of several persons. This way fingerprint information corresponding to the ten fingers of either one person, or additionally, of further persons can be stored.

For reliable verification in terms of similarity, the fingerprint information that is captured by the sensor device 'SEN' and stored can be converted into the form of a feature vector. This assumption in practice is not a limitation since the sensor data can always be depicted as an ordered n-tuple of 'n' measuring data (feature vector). The feature vectors form an n-dimensional space. In it, a set of sample vectors (codebook vectors) exists, and a distance measure (similarity measure for fingerprint features) is defined.

Each sample vector is associated with a cell in this space, which is defined in that for each feature vector in a cell the sample vector of this cell is the closest sample vector in the sense of this distance measure.

Any sample vector is associated with a control procedure for controlling the device or a corresponding piece of information for triggering such a control procedure. The determination of the closest sample vector 'f4' for a feature vector 'fe', which corresponds to the captured sensor data, thus causes a corresponding control procedure 'stp4' to be triggered, which may be executed by the aforementioned first or a second control device 'STE'. If the feature vector is not located in the cell of a sample vector, no control procedure is triggered since the similarity between the determined and stored fingerprint information is too low, i.e. the similarity does not exceed a defined threshold.

The margins for error of this method may be optimized if it has been ascertained that the feature vectors associated with the fingerprint features are sample vectors. This can be accomplished in that the system adapts to the fingerprint features during an initialization phase (codebook adaptation).

Vector quantization is not the only method that may be used in connection with the invention. Those skilled in the art are familiar with other methods, which therefore require no explanation here.

Storing fingerprint information, processing fingerprint information, comparing the determined with the stored fingerprint information and/or triggering control procedures can all occur completely or at least partially in an arrangement for controlling a device. This arrangement for control purposes can be integrated in the device or be implemented separately from the device and only be connected to the device by means of transmitting mechanisms. It is also conceivable that parts of the above-described procedural steps are performed, and/or that the corresponding hardware elements are disposed, in central devices of a communication network.

Fig. 2 shows different variations for the association of fingerprint information with control procedures in a schematic illustration. They relate to a device, which can assume different operating modes. The varying operating modes can differ in that depending on the operating mode different and/or more or fewer elements of the device are supplied with power, that different and/or more or fewer functions of the device can be executed, or that more or less restricted access to data or functions is permitted. By applying a finger on the sensor element 'SEN', the control procedure associated with this fingerprint may result in a change in the device's operating mode.

The following describes the three procedures illustrated in Fig. 2 more closely, from left to right:

Initially the device is powered off, in which state only the elements used for fingerprint recognition are turned on. When the determined fingerprint information 'fe' corresponds to the stored fingerprint information 'f1', the device is powered on by means of the control procedure 'stp1' and released for a certain person 'person1'. In accordance with a user authentication or user recognition process, this person 'person1' is granted the corresponding access to the device.

When during the next step the fingerprint 'f1' is recognized again,

the device is switched to the device profile 'profile1' by means of the control procedure 'stp113'. This may mean that, for example in the case of a communication terminal, the ringing tone volume, the admissibility of incoming calls, the ringing tone melody, the display depiction or other menu options are adjusted based on this stored device profile 'profile1'.

If now the finger 'f1' is applied again in this device profile 'profile1', the stored call number of a desired destination, such as the user's office, is input automatically and corresponding signaling procedures are initiated so as to establish the connection: dial_office.

If in the powered-off state, it is found that the determined fingerprint 'fe' corresponds to the stored fingerprint 'f68', the device is powered on and released for a person 'person2'. If thereafter the fingerprint 'f69' is detected, the device is switched to the device profile 'profile3' for this person 'person2'. If now fingerprint 'f30' is recognized, a connection is automatically made to an emergency call center.

If in the powered-off state of the device, the fingerprint 'f27' is recognized, the device is first powered on and immediately a connection to an emergency call center is initiated. If during the powered-on state then the finger 'f24' is detected, the device is switched to a general device profile 'profile1', and if a finger 'f21' is applied, the figure '0' is input on the device and, where applicable, depicted on the display.

Based on these examples the person skilled in the art will be able to implement countless other variations for associating the control procedures with fingerprint information.

Such an association can be stored during the initial use of the device in that the user selects all control options of the menu pages successively and activates each menu item by applying the desired finger on the sensor.

In conjunction with a SIM (Subscriber Identifying Module) card present in the device and/or in the arrangement for controlling the device, the fingerprint sensor may serve, not only for user recognition, but also for user authentication.

Fig. 3 shows a communication terminal KE, comprising an operator panel 'MMI', a control device 'STE', a processing device 'VE', a power supply device 'SVE', a user authentication module 'SIM', a receiving device 'EE', a transmitting device 'SE' and a sensor device 'SEN'.

The operator panel 'MMI' comprises a loudspeaker element, a microphone element, a display for depicting menu items, figures or other information relevant for a communication process and, where applicable, a keypad for inputting figures and letters and for selecting menu items.

The control device 'STE' substantially comprises a program-controlled micro-controller, and the processing device 'VE' comprises a digital signal processor, both having write and read access to the memory modules 'SPE'. The micro-controller regulates and controls all essential elements and functions of the communication terminal 'KE' and regulates the communication and signaling processes. Control procedures stored in the form of program data are read from the memory modules in the micro-controller and executed there. The control device 'STE' particularly controls when the communication terminal 'KE' assumes defined operating modes, when certain hardware elements are powered on and off, and the user recognition process.

The program data required for controlling the communication terminal 'KE' and the communication process, particularly also for controlling the signaling procedures, the device information, information input by the user, and information and reference data of fingerprint features generated while processing signals, i.e. fingerprint information of authorized users, are stored in the volatile or non-volatile memory modules 'SPE'.

In one embodiment variation of the invention these reference data or at least part of these reference data are stored on the user authentication module 'SIM'.

If the communication terminal 'KE' is a cellular telephone, the user authentication process may also be replaced by a process of comparing the determined fingerprint information with the stored fingerprint information by means of a personal identification number. After transmitting corresponding authentication data to the central facilities of the cellular phone network, the cellular telephone is logged into the cellular phone network.

Claims

1. Method for controlling a device by means of fingerprint information in which

- fingerprint information (fe) of a finger is determined,
- different pieces of fingerprint information (f1; f2;... fn) corresponding to the different fingers of a person are stored, which each are associated with a control procedure (stp1; stp2; ... stpn),
- the determined fingerprint information (fe) is compared to different stored pieces of fingerprint information (f1; f2; ... fn),
- the control procedure associated with the stored fingerprint information (f4) is triggered when the similarity of the determined fingerprint information (fe) to the stored fingerprint information (f4) exceeds a defined threshold value.

2. Method according to claim 1, in which the device can assume varying operating modes, wherein stored fingerprint information (f1; f2; ... fn) is associated with a control procedure (stp1; stp2; ... stpn) for changing the operating mode.

3. Method according to any one of the above claims, wherein the stored fingerprint information (f1) is associated with a control procedure (stp1) for executing the user recognition step.

4. Method according to any one of the above claims, wherein the stored fingerprint information (f1; f2; ... fn) is associated with control procedures (stp1; stp2; ... stpn), which are triggered when figures are input.

5. Method according to any one of the above claims, in which the device can assume varying operating modes, wherein stored fingerprint information (f1; f2; ... fn) is associated with varying control procedures (stp1; stp2; ... stpn) in different operating modes.

6. Method according to any one of the above claims, in which the device is a communication

terminal, wherein stored fingerprint information (f1; f2; ... fn) is associated with control procedures (stp1; stp2; ... stpn), which are triggered when selected information is input.

7. Method according to any one of the above claims, in which the device is a communication terminal, wherein stored fingerprint information (f1; f2; ... fn) is associated with control procedures (stp1; stp2; ... stpn), which when triggered in turn trigger signaling procedures.

8. Arrangement for controlling a device by means of fingerprint information comprising

a) means (SEN) for determining fingerprint information (fe),

b) means (SPE) for storing different pieces of fingerprint information (f1; f2; ... fn) for the different fingers of a person, which pieces are each associated with a control procedure (stp1; stp2; ... stpn),

c) means (STE) for comparing the determined fingerprint information (fe) with different stored pieces of fingerprint information (f1; f2; ... fn), and

d) means (STE) for triggering the control procedure (stp4), which is associated with the stored fingerprint information (f4), the similarity of which to the determined fingerprint information (fe) exceeds a defined threshold value.

9. Arrangement according to claim 8, comprising

a) means (STE) for causing the device to assume different operating modes, and

b) means (SPE) for storing a control procedure (stp1) so as to change the operating mode.

10. Arrangement according to any one of claims 8 to 9, comprising means (SPE) for storing a control procedure (stp8), which is used to execute a user recognition step.

11. Arrangement according to any one of the claims 8 to 10, comprising means (SPE) for storing control procedures (stp1; stp2; ... stpn), the triggering of which corresponds to the input of figures.

12. Arrangement according to any one of the claims 8 to 11, comprising means (SPE) for storing control procedures (stp1; stp2; ... stpn), the triggering of which corresponds to the input of selected information.

13. Arrangement according to any one of the claims 8 to 12, comprising means (SPE) for storing control procedures (stp1; stp2; ... stpn), the triggering of which corresponds to signaling procedures.

14. Cellular telephone comprising an arrangement according to any one of the claims 8 to 13.

3 pages of drawings

FIG 1

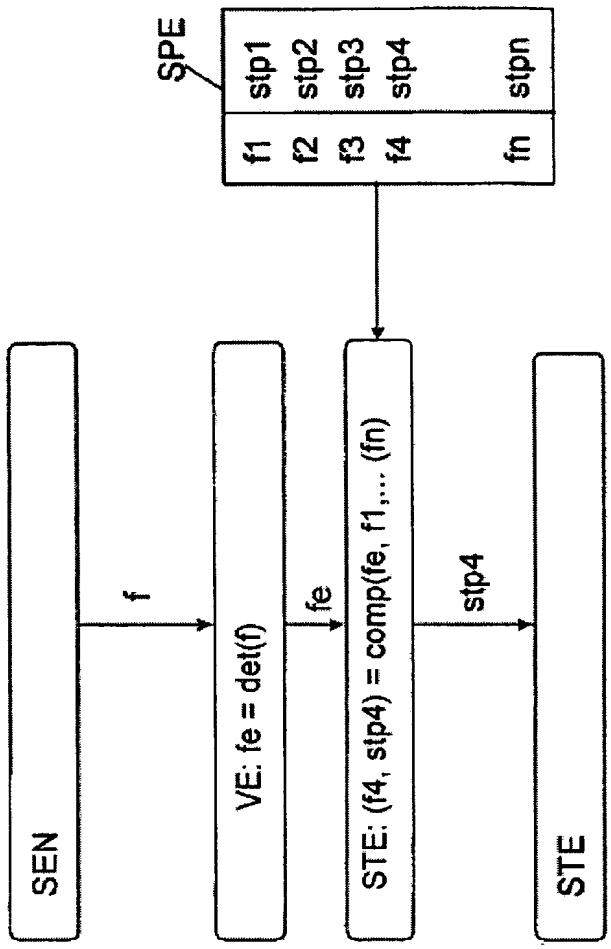

SPE
stp1
stp2
stp3
stp4
stpn
f1
f2
f3
f4
fn
SEN
f
VE: fe = det(f)
fe
STE: (f4, stp4) = comp(fe, f1,... (fn)
stp4
STE

FIG 2

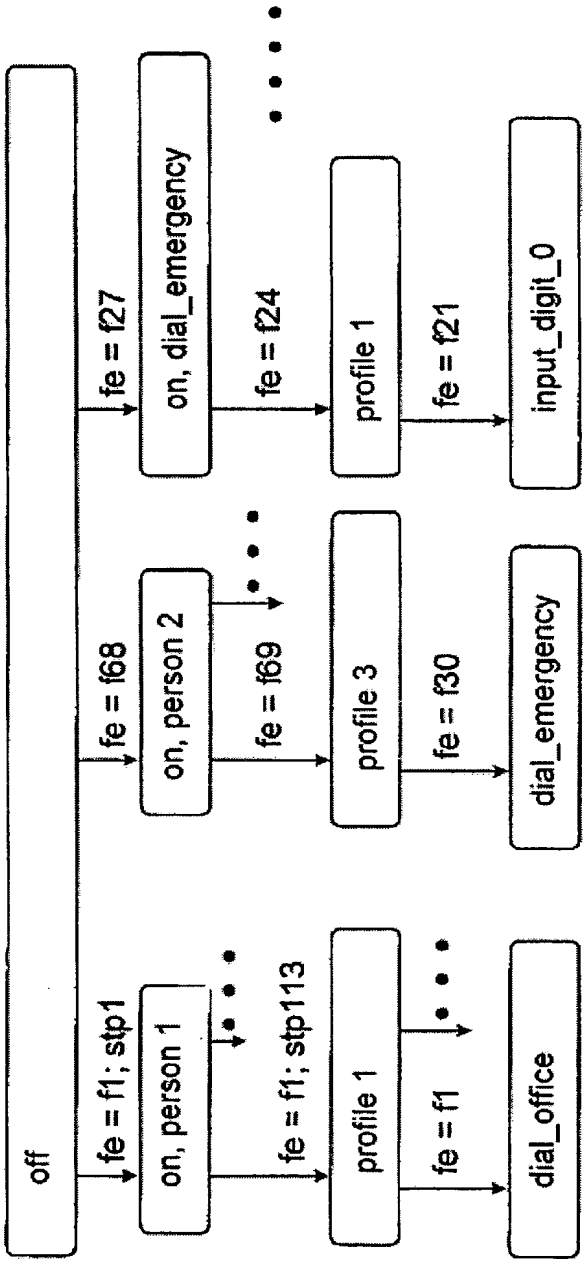

off
fe = f1; stp1
on, person 1
fe = f1; stp113
profile 1
fe = f1
dial_office
fe = f68
on, person 2
fe = f69
profile 3
fe = f30
dial_emergency
fe = f27
on, dial_emergency
fe = f24
profile 1
fe = f21
input_digit_0

FIG 3